## SECURITY SUITABILITY OF APPLICANTS

It is unstated but implicit in the tasking that current security standards for applicants and employees should be examined in the light of realistic criteria. The issue is valid; there has been a profound change in national social values over the past thirty years and it is entirely proper to determine whether or not the Office of Security has reacted in a manner and to the degree that is consistent both with staffing requirements and the Office's mission to prepare and execute an effective Agency security posture. In seeking determination, it is not necessary to detail the dramatic change in social mores over the past three decades. It is enough to say that the traditional values of the 1950s were challenged in most dramatic fashion in the 1960s and evolved in the 1970s and 1980s, with some positive reaction to extremes, to the climate of today. The net result of rebellion, activism, revolution within the ethical and moral infrastructure, hedonism represented in self-gratification and overriding self-interest and the many other expressions of societal change have resulted in:

- Selective patriotism.
- If not rejection of authority, then at least suspicion of it.
- A search for meaning involving both a return to some traditional values and a proliferation of cults that exploit a need for direction.
- Weakening of the family structure.
- Development of a drug culture particularly in the young.
- Cohabitation as a generally acceptable alternative to a "legal" union.
- A relaxed attitude toward casual sex.
- Selective observance of law.
- An attitude held by many that cheating and some forms of theft are justified to satisfy personal need.
- Emergence of the overt homosexual and some acceptance of deviant lifestyles.
- Polarization on political, religious and moral issues.
- Peer examples, attitudes and the age factor

25X1

place most applicants in the group likely to have accepted those societal changes that conflict with security criteria; e.g., use of drugs.

There are, of course, many other changes not listed above, some bearing on security criteria and others dealing with suitability factors. At this point, it is important to establish the distinction between information relating strictly to security (loyalty, integrity, criminal record, etc.) and other developed information that concerns fitness and overall suitability not necessarily related to security decisions (family background, stability, personality quirks, etc.). The distinction figures prominently in a discussion of counterintelligence presented later in this paper. The separate criteria also are significant if unstated in the review set forth immediately below.

The Office of Security does not operate in a vacuum and would not if such an insular condition was possible. Reality dictates flexibility in application of security standards to the degree the mission of the Agency is not jeopardized and, within this limitation, change has occurred. Examples:

- Cohabitation, once disqualifying under provisions of Executive Order 10450, no longer is a basis for security disapproval. There is security interest in a partner with spouse-like status in terms of identification. We require some reasonable assurance that a cohabitant who enjoys the same confidence given to a "legal" partner is trustworthy. Such assurance is not always available because partners tend to come and go and there is no effective mechanism for keeping current of temporary "relationships." The Office has chosen to accept the risk associated with the nature and pattern of cohabitation because there is nothing to do but to accept and live with this particular element of an altered public attitude toward sex and sexual unions.

- The definition of promiscuity, which under Executive Order 10450 represented "notoriously disgraceful conduct" has been modified to conform to relaxed public perception of sexual behavior. Sexual activity is not disqualifying unless it is flagrant to a degree to embarrass or discredit the Agency.

- Experimentation with drugs, as it figures in the adjudicative process, essentially involves judgment as to whether or not an applicant can avoid use of drugs after entrance on duty.

The Office is acutely aware that failure of individuals to meet security standards often deprives the Agency of the services of people well qualified in the professional sense. We also are aware and very much concerned over a heavy incidence of security-related terminations in the past few years. In discussion of these matters, internally and formally and informally with the Office of Medical Services (OMS), the following questions have arisen:

- Are our clearance standards realistic? Have we become institutionalized to a degree where regulations and policy dictate criteria that are too rigid and not in keeping with the times?

- Are our security standards valid and sound; that is, are they based on internal perceptions not supported by study that confirms their viability?

- Are our adjudicators sufficiently knowledgable of suitability factors that warrant referral to the Applicant Review Panel?

- Do our security standards contribute negatively to the overall quality and professionalism of the Agency populace? In simple terms, are we rejecting people who can do the job and clearing less gifted and talented men and women who require extensive development before they can function effectively? If the latter is true, are we conducting a social experiment to the detriment of the Agency mission?

- Must we accept as fact a premise that the best and the brightest in today's job market are more likely to have accepted moral and ethical standards incompatible with current security standards? On the other side of the coin, are people who are governed by high standards of personal integrity and reject the drug culture necessarily second rate clods who have only their virtue to recommend them?

- Does the recent spate of security terminations indicate that existing security standards for clearance already have been weakened to the point of intolerance?

Before addressing these questions it is necessary to establish the points that may or may not be approached as within the Office's authority. Two major issues, homosexuality and drug usage, are governed by Agency rather than Office of Security

policy. The Office of Security has the lead in recommending policy, but it must be affirmed by the DCI. Briefly, overt or practicing closet homosexuals are not eligible for Agency employment; those who start or continue using drugs illegally after entrance on duty are not eligible for continued employment.

The questions raised obviously call for a good deal of soul searching and applied analysis. This is, of course, a continuing process that calls upon past experience, the lessons of the present, and a constant evaluation of changing societal values that influence applicants. Our conclusions:

- We are not insulated nor do we act in accordance with rigid and inflexible standards. We cannot deny an institutional influence, but this very influence features awareness of and reaction to societal evolution.

- Internal perceptions are valid because they are not locked into the past and conform to the Office obligation to avoid unacceptable risk. The Office has made adjustments in security criteria and it is possible other changes may justify themselves or be imposed upon us. We would have no objection to a study of today's society and its values vis-a-vis current security standards but contend such a study would be no more than an extension of or appendage to ongoing practice.

- The expertise of our adjudicators in suitability matters should be expanded and supplemented. This matter is dealt with at length in a discussion of counterintelligence presented later.

- The question of whether or not we are rejecting well qualified people at the expense of the Agency's ability to fulfill its mission is not for the Office of Security to judge. We obviously do not recruit and select new employees other than our own and other components must judge the quality of their personnel. The matter should be explored thoroughly with consideration of all factors that contribute to the effectiveness of the Agency work force and problems, if any, should be discussed by heterogeneous Agency representation, including this Office.

- Relating to the question addressed above, the Office of Security has not found in its recruiting efforts that all or most of our

clearable applicants are marginal or sub-standard. High quality personnel are harder to find but enough can be located to maintain a pool of high potential professionals. In our experience, this demonstrates the variance in contemporary society; not all of the bright and capable young people accept the values of an apparent majority of their peers. Accepting this, the issue becomes a necessity to investigate and process more people to fill a need and not modification of existing security standards.

- The number of terminations on security grounds in recent years is most disturbing as a possible indicator that security criteria has already been relaxed too much. Some employees who experimented with drugs before entrance on duty and were advised of Agency policy on illegal use of drugs did not heed the warning. In several instances, cocaine replaced marijuana as employees became able to afford the more expensive substance. There was a marked increase in demonstrated dishonesty which seems to be symptomatic of a growing trend influenced sometimes by a tight economy and other times by a plain lack of concern for this element of character. Other cases involve sexual deviation. There is no apparent pattern to these terminations except that most surface during probationary polygraph and reinvestigation. At this time, it cannot be stated if the several terminations are an aberration or related to security and/or suitability factors. The matter should be pursued internally in coordination with OMS.

All security criteria are geared to the counterintelligence function of protective security. As society becomes more complex and the influence of societal change more evident in the conduct and attitude of the citizenry, it has become increasingly apparent that security and suitability factors are becoming more and more interrelated. There has never been a sharp delineation between the two criteria and this is proper as evidenced in inclusion of emotional and mental problems in DCID 1/14 adjudicative guidelines. Now, however, our counterintelligence specialists who deal with espionage and other classic counter-intelligence problems cite the direct relationship between such problems and "suitability" issues involving personal behavior. For example, a history of poor adjustment to employment or educational environments, difficulties in interpersonal relationships, a penchant for risk-taking, reluctance to accept discipline, among many other forms of psychological dysfunction, should all be regarded as indicators of possible trouble to

come. In effect, security has become inexorably married to psychiatry.

Within the Intelligence Community, the DCI Security Committee has made an effort to reach accommodation between security clearance standards and internal/external social pressures through a series of adjudicator conferences. The effort has suffered because of the absence of expertise and knowledge of security personnel when dealing with psychological dimensions of suitability problems. Adjudicators cannot be expected to know and understand the language of psychology, much less detect and evaluate the subtle shadings of background meaningful to a psychologist or psychiatrist. The need for continued dialogue in this area is apparent. It is unrealistic to expect security personnel to qualify as experts in detection of counterintelligence-related behavior and psychological indicators, but we must become more familiar with significant if basic dimensions of suitability problems. The answer lies in two directions, increased reliance on OMS and a serious effort to open up those avenues of education that will permit exploitation of a related discipline.

In summary, the Office is completely aware of the dramatic changes in societal values over the past 30 odd years and, of necessity, has reacted to them through change in significant areas such as cohabitation and experimentation with drugs. We do not believe present security criteria are oppressive and counterproductive in terms of tunnel vision, institutional intransigence, empirical conviction or failure to implement reasonable revision of security standards. We are concerned about the possibility that the quality and performance of the Agency populace may be deteriorating because of the necessity of disqualifying many promising prospects who fail to meet security standards; however, we are not convinced on the basis of our own recruitment efforts that qualified applicants necessarily are inferior to those who live in the fast lane with respect to drugs, a self-serving concept of integrity and other behavior found in those "with it." Admittedly, it is harder today to find the people who meet our standards, but it can be done. Our concern also extends to the possible implications of already relaxed standards raised by a heavy incidence of terminations for security reasons. Are we already too lenient and have we sacrificed the long-term benefit of good character for short-term expediency? This question should be studied in depth. At the same time, the Office should initiate or be involved in a thorough review of the feasibility of exploiting psychological and psychiatric analysis in screening applicants in terms of counterintelligence-related factors with which our adjudicators cannot cope because of lack of expertise and a less than optimum working relationship with OMS.

In conclusion, we see a fundamental conflict between today's values and lifestyles that may be incompatible with the high personnel security standards requisite to operation of an intel-

ligence agency which may be irreconcilable. Within the framework of contemporary mores, there can be only so much compromise. An Agency employee must be trustworthy in that he or she must be loyal, with a depth of loyalty that extends beyond payment for services rendered; responsible to the degree it is appreciated illegality and dishonesty cannot be tolerated; disciplined from within to avoid excesses and thoughtless self-indulgence; and stable enough to handle transient disappointments, frustrations and the pressures of a unique work environment and demanding assignments. We cannot:

- Accept the explicit lawlessness represented by the purchase and use of drugs beyond the experimental stage.

- Place "experimentation" with hard drugs (including cocaine) in the same category as former use of marijuana.

- Tolerate disregard for honesty in personal and professional affairs.

- Dismiss emotional problems or indicators of such problems as not related to security screening. Indicators of a potentially serious problem developed during security screening or reinvestigation must be made known to OMS and referred to the Applicant Review Panel or Personnel Evaluation Board.

We must:

- Maintain an adequate security posture through selection and retention of trustworthy and stable individuals.

- Exploit the assistance available from specialists in psychology and psychiatry by training of our adjudicators to the extent possible in the disciplines and utilization of the expertise to be found in OMS and the medical community.

- Continue monitoring of societal change in terms of acceptable revision of security criteria.

- Reject a concept that security criteria must be an absolute mirror of contemporary values and practices. There are constants in determinations of loyalty and trustworthiness and they must not be violated to accommodate permissiveness incompatible with the basics of overall suitability for Agency employment.

- Not lose sight of the importance of our role and mission as it depends on the honesty and reliability of our employees. This translates to high security standards, some of which conflict with today's ethics.

- Given the last point, accept the fact that recruitment and the related screening process has become more difficult. We must screen more people to find those who meet our standards, be they security criteria or professional credentials.

- Direct our energies and resources to finding and keeping the people we need. This will involve many considerations including incentive to sign on, the efficacy of the present recruiting system, dedicating the resources to gain a substantial decrease in applicant processing time, and a comprehensive study of the present policies on training, promotion and other recognition as these factors bear on retention.

To capsulize the Office of Security position, we see no need for drastic modification of security standards and policies. Security criteria has evolved just as societal mores have evolved. The process will continue, but only to the limit of tolerance that can ensure a sound security program. We cannot condone demonstrated illegality and dishonesty and we maintain there is little room for more concessions except at the risk of secure operation. We regard the factors that figure in security adjudications as essential to counterintelligence both in the near and long-term; our immediate concern is to gain a sophistication extending beyond expertise in pure security issues to the related psychological and psychiatric aspects of character and behavior. The Office submits that its own experience in recruiting professionals negates any perception that security criteria deny the Agency the services of the best and the brightest. We do not live in a homogeneous society and it is fallacious to believe that all promising young people accept the drug culture and other unacceptable facets of today's scene. Admittedly, it is harder to find and hire people who meet our professional standards and security criteria, but difficulty should not govern selection. We strongly oppose any quick fix that would diminish the Agency's security posture and lead to a succession of future problems. In our opinion, the nature of the Agency's mission demands that security be optimum and precludes lowering of personnel security standards which above all else contribute to a secure operation or the lack of it. The answer to immediate problems associated with staffing lies in elimination of the factors that represent negatives in the recruitment

and retention of the type of people essential to effective and secure discharge of the Agency's mission.

## POLYGRAPH EXPANSION

As we understand the tasking, initiatives are to be proposed that will permit an immediate capability to reduce or eliminate backlog of polygraphs, particularly in applicant screening, industrial cases and reinvestigations. Before dealing with supplements to existing corrective measures, a review of accomplishments resulting from ongoing Office initiatives is in order to permit evaluation of their effectiveness. Among accomplishments:

- The CIA Polygraph School has graduated its first class of four. These individuals are at least three months ahead in their contribution to the Polygraph Division's mission than they would be if trained in a commercial school. The CIA Polygraph School, certified by the American Polygraph Association, must be considered a success beyond the most optimistic estimate of potential during planning and development.

- The waiting period for applicant cases has been reduced to slightly over 30 days. This effectively eliminates the polygraph as a major roadblock to timely processing of applicants.

- Reinvestigation polygraphs this fiscal year are being conducted at a rate of five times our production for last year.

- Probationary polygraphs are up 40 percent.

- Operational polygraphs are up 20 percent.

- The above gains are all the more significant in light of the fact production in fiscal year 1982 was one of the highest in our history.

The impact of ongoing initiatives is obvious, encouraging and, in our opinion, a strong support for an argument that the solution is at hand given a reasonable time to train and activate additional polygraphers. Application of short-term heroic measures would gain immediate results, but at a cost we do not feel is acceptable. To illustrate this point, specific weaknesses associated with alternatives are presented below.

Utilization of a Commercial Firm. This is not considered a desirable option in any form. Commercial polygraphers are not trained in the CIA methodology and their use would require either the time and expense attendant to retraining or turning them loose to explore areas they are not equipped to handle. In either instance, their value would be limited. We consider it entirely inappropriate to expose our employees and contractors to the scrutiny of commercial polygraphers in the Reinvestigation Polygraph Program. Employees and industrial candidates are people who have had access to very sensitive information. The issues that examiners must probe in resolving reactions, particularly when dealing with unauthorized disclosure and mishandling of classsified information, involve highly sensitive areas; they (the examiners) require compartmented approvals. Good security practice demands that exposure to our most critical intelligence data remain in-house.

Quality control, directly related to the validity of polygraph examinations, will suffer beyond the point of tolerance; commercial polygraphers are geared to production and minimal operating costs. The pressures of this approach preclude the extreme patience our examiners must display to pursue and obtain complete and accurate information. The commercial polygrapher is given to quick judgments and early dismissal of subjects based on reactions. From the professional standpoint, this is incompatible with the validity of broad screening tests.

Representational aspects would not be served by use of commercial polygraphers. The polygraph is highly intrusive, and for this and other reasons inherently a controversial activity. The Agency has respected this in years of circumspect screening of Agency applicants and employees, and has gained a relationship with its contractors reflective of a long-standing, carefully nurtured and understanding position. All of this would be jeopardized by use of polygraphers hired as transitory help and completely disinterested in the long-term consequences of heavy-handed questioning or other unpleasantness avoided by our staff polygraphers.

Commercial examiners are not schooled in counterintelligence issues. This alone is regarded as an absolute negative in measurement of their use as an expedient.

Independent Contractors. We have explored the use of individuals who could serve in the short-term as Independent Contractors and the experiment produced mixed results. One Agency annuitant agreed to participate, but only for so short a time that his contribution had no appreciable impact on the workload. There are not enough Agency annuitants with state of the art expertise and knowledge of current techniques (to say nothing of willingness to participate) to reduce existing backlogs to any significant degree. Essentially, use of Agency annuitants is not a viable option.

We are, with some misgivings, about to experiment with two annuitants from other agencies. Our misgivings concern the need to train the prospects in Agency methodology and the fact that training and supervision are contrary to the concept of "independence" as defined in the legal sense. Quality control might present a problem, as might motivation and the aforementioned representational aspects. As with Agency annuitants, retirees of other agencies who are qualified and able to serve as polygraphers are in short supply. The Office is open-minded at this stage of the experiment and will pursue it if the two prospects perform well.

Joint Efforts With Other Government Agencies. The few Federal agencies with a polygraph program have fully committed their resources and, with the signing of the new directive addressing containment of leaks, will almost certainly be forced to cope with an increased workload. Even if other agencies could divert resources, we would face the problems concerned with incompatible training, quality and lack of control of an element of our polygraph program. Other agencies would have the same problems in any joint effort and, even if we could support other agencies with already strained resources, it is probable they would be less than enthusiastic over the prospect. Joint effort as a concept is not practical.

Past experience has lead to rejection of other options that have been proven impractical. They are:

° Overtime. Polygraph as a discipline features pressure, stress, and mental and physical fatigue. Any use of overtime on other than a very limited basis is a negative in terms of test validity.

° TDY assignment of former polygraphers. Polygraph examiners are volunteers who serve at least a four-year tour. Without constant practice of polygraphy, former examiners do not maintain the level of required expertise. Temporary reassignment of Polygraph Division alumni would be contrary to the understanding between office and employee governing assignment as a polygraph examiner and, in the first instance, would be unproductive. Beyond the fact it would take time to bring former examiners up to speed, they cannot be removed from primary duties to the detriment of core functions.

° Creation of a reserve polygraph corps. Years ago (circa 1960), the Office trained professionals to serve as a backup to dedicated polygraph examiners. They received initial training and periodic refresher training, and supplemented the full-time polygraphers on

occasion, usually by running apparently "routine" cases. The idea was dropped when it became apparent part-time polygraphers had to be prepared to cope with difficult/involved cases (there is no guarantee any examination will be "routine"). The required level of expertise could not be reached with a part-time commitment. In the future, the capability offered by in-house training may permit consideration of some modified version of the old program, but now is not the time. We cannot tie up resources of the Polygraph Division on a questionable experiment when faced with the present workload.

In summary and conclusion, the Office believes that production in this fiscal year has diminished backlog considerably and justifies optimism of continued progress. Ongoing initiatives which figured directly in growth of production are believed to have been proven as a long-term solution. None of the options mentioned as candidates for short-term relief hold the prospect of success and some, particularly contracting out to commercial firms, are unacceptable in terms of utility or feasibility. It is our conclusion that the answer is in hand. Allow a reasonable time for the development of additional polygraphers trained in our methodology and motivated to meet our standards, and we are confident that the challenge will be met and quality will remain high. It is our conclusion that expediency must not dictate acceptance of dangerous or unrealistic emergency measures. It is our recommendation that we be permitted to stay on the course of internal improvement represented by the success of the current program, i.e., graduated additives to Polygraph Division's resources. The key to expansion that will permit full and timely service is the rate of expansion permitted by the budget process.

## REVITALIZE AND EXPAND THE EMPLOYEE SECURITY AWARENESS PROGRAM

The tasking acknowledges that a security program exists but does not note that the program represents comparatively recent formalization and significant enhancement of activity in the security awareness field. In effect, we have been asked to comment on an ongoing program in terms of additional emphasis and improvement. Revitalization is not appropriate to the paper; the current program is vigorous, effective and a successful initiative within the limits of staff, plans and equipment.

The Security Education Group (SEG) is charged with the operation of the Agency's security awareness program for employees. The staff includes five professional security officers, three of whom (non-supervisory personnel) bring a level of limited experience to the job consistent with the youth of a preponderance of Office professionals; i.e., they are conversant with the full-range of Office of Security functions but generally lack the hands-on experience in the several security disciplines.

The existing program could be improved by extensive refurbishment of the facilities now used for briefings and by acquisition of additional training facilities. The storage facility in Room GA-13 should be vaulted to permit less time devoted to security housekeeping and for solid security reasons involving the safeguarding of classified media used in briefings. Both rooms need attention to heating and air conditioning equipment and extensive internal improvement in equipment and decor to facilitate media assisted briefings and generally provide an atmosphere conducive to learning and representational of the seriousness of subject matter. The Office has reprogrammed $40,000 to refurbish GA-13 in FY 1983; this will satisfy the most immediate and pressing need.

The present security awareness program features two primary elements, the 1 ½ day EOD briefing and the "reawareness" sessions of one to two hours tailored to the needs of the various Agency components. The last mentioned sessions represent an innovation that reflects commitment to periodic reminders of security responsibility. They have proved valuable in that employees who have been on board for some time are given the opportunity to raise questions on security standards and practices of particular interest to them as individuals or as members of a group with unique problems. There is a good deal of give and take in these sessions because they deal with people who have been on the job and have their own ideas on the merit and efficacy of security procedures. This is in contrast to EOD briefings where attendees generally are new to the Agency and to Government and are not in a position to do more than sit and listen. Obviously, both the EOD and "reawareness" briefings are valuable and, in fact, indispensible to understanding of what is expected of the employee in order to comply with security regulations. Any

expansion or improvement of the security awareness program would focus on improving the quality of both types of briefings.

Any serious effort to improve the security awareness program would involve:

- Development of a reindoctrination format to permit more frequent briefings on security obligations and responsibilities.
- Funding to create new audiovisual programs.
- The aforementioned refurbishment of existing plans, plus the acquisition of another briefing room properly equipped and furnished.

The above listing represents resource enhancement which would permit a quantitative but not necessarily a qualitative gain in the program. The briefings would benefit from inclusion of actual case examples of recent and significant physical security violations, careless or negligent handling of classified information, leaks and their consequences, and hostile penetration attempts. These case studies could be prepared by the Office of Security component(s) involved in a given case and sanitized and depersonalized in the manner appropriate. There are many dramatic lessons to be learned from our experience in dealing with and measuring the consequences of breaches of security and hostile operations; these lessons are more meaningful when presented as immediate examples of the impact of poor security practices.

Another approach of potential value, particularly in EOD briefings, is the filming of especially well-done presentations. The advantage of this technique lies in assurance that a comprehensive and smooth informational talk is available to supplement in-person briefings. Films cannot replace live briefers; they cannot answer questions or address any concern of the viewer that strays from a script. Films are, however, a change of pace that breaks whatever monotony is associated with a steady stream of speakers.

Films also are used as a briefing device in the form of dramatization of security hazards associated with loose talk, cultivation and exploitation by the opposition, the damage caused by leaks, etc. The problem with this approach is audience reaction if a production is poorly directed, played by obvious amateurs, and simplistic in presentation of complex issues. The medium generally is not effective in providing specific guidance that reflects regulatory obligations and responsibilities; it is most effective in presenting a broad picture of generalized security concerns and, in this regard, is as much entertainment as indoctrination. There is some benefit if the film is well written, directed and acted and does not insult one's intelligence in making a point. It must also be current; viewers do not

relate to object lessons obviously prepared for an earlier time and audience. At present, the Office of Security has no up-to-date dramatization available that was sponsored in-house. We do not contemplate preparing a film in the near future because of budgetary considerations. This, however, does not preclude planning for a quality production if and when funds are available.

SEG plans to expand the use of audiovisual aids other than films to supplement briefings by staff members. Slides and graphic illustrations are proven educational tools and figure as a major item in raising the level of attention to and retention of subject matter presented in live briefings.

There is no guarantee that well equipped SEG staff can insure responsible adherence to security regulations. To the contrary, raising security education to a group speciality and introducing a matrix of penalties set forth in HR 10-11*, Compliance with Security Regulations, has not been completely effective in eliminating a frustrating and nagging problem bearing on improper handling and storage of classified information. Despite these measures and unannounced briefcase/package inspections, Agency employees persist in taking classified information out of the building and working on it at home. The violators are not malicious people who wish harm to the Agency and their transgressions in one sense are indicative of dedication. Their enthusiasm is misplaced, however, when weighed against flagrant disregard of security regulations and the risk of compromise.

Another approach to security awareness illustrates the line responsibility inherent in achieving compliance with all security regulations by the Agency populace. The Office of Development and Engineering (OD&E) recently published a comprehensive security indoctrination manual which covers both Agency and SCI policies. The manual will be used by OD&E security officers to conduct an annual security indoctrination of all OD&E employees. This initiative could serve as a model for all Agency components and as a most valuable adjunct to SEG activities. OD&E has a large complement of security officers to assist in security control of national programs and this undoubtedly contributed to the initiative. We do not advocate an increased Office of Security presence in all components but note in-place security officers have a direct bearing on good security management practices. For our part, we welcome security-oriented innovation as appropriate to a high level of security consciousness. Security is a command function that looks toward observance of security policy and practice established by the Office. The concept of component participation is entirely in line with an effort to upgrade security awareness.

The tasking specifies that publicizing security violations should be examined as a device to enhance security awareness. The Office of Security recognizes possible benefit from an

approach that might bring and keep security awareness to the forefront of employees' consciousness. We are reluctant, however, to endorse the concept without full understanding of scope and intent. This concern involves protection of polygraph-derived information, the feasability of publishing a completely depersonalized report, and misgivings regarding the integrity of security information which by regulation receives extraordinary protection and extremely limited dissemination. We would prefer and recommend a method other than a "newsletter" approach to bring the message home before a serious effort to implement the concept.

In summary, the Office believes that the SEG function can be enhanced by providing additional material resources, upgrading audiovisual presentations, and in general improving the SEG product in terms of currency and relevance. As an adjunct to SEG activities, we recommend the approach reflected in the cited OD&E publication. At this time, the Office does not favor publicizing security violations as a phase of the overall security awareness program.

# TERRORIST THREAT

DOMESTIC

In today's climate, the terrorist threat as it applies to Headquarters and other open Agency facilities should have diminished upon the demise or limited activity of the weathermen and other underground groups. The threat, in fact, remains as a serious potential hazard. The organized terrorists have been supplemented by deranged or disturbed people who have embraced a variety of causes and are willing to take extreme risks for the sake of publicity, an unreasonable commitment to a movement, or the several other motivating factors that figure in irrational acts. In addition, organized terrorism is still a threat; while attacks against the establishment by radical activists and attempts to disrupt Government by extremists and their supporters are less frequent, there has been no decrease in the number of political fanatics concerned with foreign issues who are capable of seeking redress or publicity through violence. The following represent obvious threats:

° A demonstration organized without intent of violence that, through the efforts of provocateurs, degenerates into a riot and/or attack on Agency facilities. Unless infiltration by a hostile element is sufficient to displace the organizers, this type of occurrence should be contained by local or Federal police quickly and without extensive harm to person or property.

° A bombing attack. Such an attack is possible with only a moderate degree of technical expertise and preparation. At Headquarters, with the protection of badge machines, it is probable that a bomb would be placed somewhere in the compound, set to give the perpetrators time to get away, and exploded in an area where casualties and damage would be minimal. This type of attack is the most likely because it involves little immediate danger to those involved, and still would serve to gain a great deal of publicity.

- A bombing attack on an outlying building could have more serious consequences. Without the protection of badge machines, entry with a forged badge would not be difficult and a sizable bomb could be placed for delayed detonation. A bomb could also be introduced into an outlying facility for use in hostage and/or takeover situations.

° Assassination. An assassination attempt can involve either a target of opportunity or a determined and planned effort to kill one or more well-known figures either held personally responsible for perceived wrongs or selected as symbols of an objectionable system or practice. An assassination can be attempted anywhere and, therefore, protective measures cannot be confined to Agency facilities. They may be the result of impulse usually involving the deranged, or could be carefully planned and organized, calculated attacks. In either instance, warning is unlikely and prearranged countermeasures an absolute essential.

° Armed attack. Attack by a group of trained terrorists could be mounted for a number of reasons, including the theft of classified information, the taking of hostages, a staged takeover that would be assured of immediate and extensive media coverage, or a suicide mission by fanatics determined to publicize a cause. Whatever the motive, the present system of guards, entrance control and backup capability is not geared to stop a well organized terrorist attack either in the training given or physical security safeguards.

° Surreptitious forced entry. It would not be difficult for one or more professional terrorists to gain entry into Headquarters buildings. Entry into the outlying buildings would be even less difficult. Once inside a facility vaults and safes would slow but not stop forced entry; safekeeping devices cannot be made invulnerable and can only delay knowledgeable efforts to defeat them.

Our protective security no longer is consistent with the environment in which we live and work. It is conditioned by a complacency deemed inappropriate to the mission of an intelligence agency and a perception that the impact of tight physical security would be negative and self-defeating in terms of production, extensive liaison, required maintenance and the purpose of visits. We aim for adequate and not absolute security. It is

possible to secure our facilities and grounds by duplicating prison-like security arrangements featuring such safeguards as unscalable walls, barred windows, heavily armed guards, impassable internal gates and doors, sealed areas and all of the other devices appropriate to containment of a criminal population. Such extreme measures are not, of course, either feasible or necessary, any more than overseas embassies built like castle keeps are acceptable. Another negative factor is prohibitive cost in dollars; in this area monetary cost must be balanced against the loss that would be experienced as the result of a serious incident.

The Office of Security has established procedures to follow when a terrorist threat or attack is reported. These procedures, attached, illustrate the limited resources and protective measures available even in a "red alert" when the reserve of available manpower is tapped. Essentially, the Agency must depend on the FBI and local police to protect against a terrorist attack. Existing safeguards can be enhanced with moderate expense. Such enhancement would not gain self-sufficiency, but would go a long way toward adequacy. Areas that must be improved include:

° Better screening of visitors through a Headquarters Visitor Control Center. This is a key need.

° Improvement of building security through placement of badge machines in outlying buildings.

° Enhance Headquarters security at the perimeter through improved fencing, gates, and lighting.

° Development of a more secure badge.

With or without enhancement, there are built in weaknesses and some significant strengths in existing physical security countermeasures. On the positive side:

° Officers assigned to protective security of high Agency officials are armed, qualified in the use of weapons, and trained in techniques utilized by the Secret Service.

° It is probable that screening of visitors would detect an unstable individual. The chance of detection would be greatly enhanced by screening at the perimeter.

° The presence of Federal Protective Officers affords the power to arrest.

° With warning of trouble, we may call local police for assistance on short notice.

° The Federal Protective Service can provide an impressive display of manpower and adequate protection in the event of demonstrations, unless they are spontaneous or unannounced.

° The Office of Security can arm and deploy personnel to supplement the Federal Protective Officer complement.

° Existing safeguards discourage trespass. They look more effective than they are.

On the negative side:

° The absence of badge machines in outlying buildings increases the risk of unauthorized entry.

° Access to the compound, with or without a badge, cannot be controlled in a manner consistent with optimum security. This problem, created by a need to handle a large traffic flow at peak hours, will be more pronounced after completion of the new building.

° Existing security precautions are most effective with warning. All such precautions are, to some degree, dependent on a lack of surprise.

° We have neither the people nor the firepower to repel a well organized and planned terrorist attack, undertaken with modern weaponry.

° Excluding those certified for protective assignments, our Headquarters personnel are not trained to prevent or protect against planned attack.

° As already stated, physical security safeguards were not established to properly deter an armed attack. It is not believed possible to set up an adequate defense without adopting a fortress mentality inconsistent with the manner in which the Agency now does business.

The existing physical security safeguards accomplish what they were intended to do; ensure that routine entrance and egress concern or are related to official business. They were, quite frankly, conceived in a benevolent environment with provision for emergencies that could be handled with our own resources or, in exigent circumstances, by law enforcement agencies. The approach

was dictated by the decision to go public with the location of Headquarters and outlying buildings and the resultant need to accommodate operation in a fishbowl. These measures have worked, but only to the degree they have not been tested. Gaining absolute security is impossible as a concept and, more to the point in this exercise, would be both cost prohibitive and an unacceptable bottleneck to the pursuit of the Agency's business. Some improvements are needed and they have been identified. Measurement of whether or not cited improvements will suffice in the face of a threat requires analysis of the threat. These factors apply:

° The Agency has survived to date without suffering a serious domestic attack by terrorists, excluding the bombing of the Office of Security's New York Field Office. The latter incident may not have been aimed at the Agency; instead the target might have been the Department of Defense. In any case, the bombing illustrates vulnerability when well organized terrorists choose a target.

° The security of Headquarters and outlying buildings in the Washington, D. C., area include protective measures that cannot be used in a cover situation such as existed in New York. Fences, perimeter guards, and controlled entrance into the buildings or that portion of them occupied by Agency personnel represent a level of security well above that afforded other Government facilities, the National Security Agency and military establishments excepted. Improvements or expansion of fencing, visitor control, and use of badge machines will raise the level of physical security without significant impact on the Agency's day-to-day operations.

° Our liaison with the FBI and Secret Service has been effective in alerting us to danger represented by group or individual activity. With warning, security protection can be enhanced to a level of counterforce adequate to deal with unfriendly demonstrations and/or armed attack.

° So long as we have outlying buildings, defense of the people and material therein will be difficult. Perimeter security at these buildings necessarily cannot be as visible and effective as at Headquarters. The visibility of control measures in itself is a deterrent.

° A factor in planning an attack is the probability of getting out as well as getting in. Entrance to any of our open facilities would

be comparatively easy and, as stated, we could not stop a surprise armed attack if outmanned and outgunned. However, once the element of surprise is gone, attackers would have difficulty in escaping and could not hope to resist a siege. This narrows the type of armed attack that might be attempted. Only groups or individuals who are willing to accept the consequences of their actions would accept the risk.

° We do enjoy a home country advantage in that we do not have to depend on politically oriented response or the lack of it from the security forces of host nations.

° Risk must be accepted when Headquarters building is an area tourist attraction, so long as our outlying buildings must limit protective security measures, and when most of our employees are open and, therefore, a potential target for any person or organization bound to register a protest against the Agency and its activities.

° The record so far is encouraging in any estimate of the probability of terrorist attack. The fact that local buildings have not been hit is not, of course, a guarantee they are immune from attack. Whether our good fortune is related to the Agency mystique or if terrorists have decided other targets suit their purpose, the fact remains that the Agency has been spared. Even without a guarantee history cannot provide, this is a factor in an estimate of adequate enhancement. In our judgment, identified improvements and additions represent a reasonable approach that recognizes we cannot button up to a point approaching invulnerability.

In summary, the threat of terrorist attack to Headquarters and outlying buildings exists as a distinct possibility. The most likely danger involves demented or disturbed individuals; present security measures should negate this threat. We are vulnerable to an organized terrorist attack, but the cost of installing elaborate barriers would be prohibitive and inappropriate to the manner in which the Agency has chosen to operate. Organizing and equipping a "SWAT" team to defend or reclaim a building would not be productive. Such a team could not respond in time to defeat a well organized attack mounted with split-second timing. After forced entry, local police would be at the scene and would operate with a professionalism expected of specialists. On an historical basis, existing safeguards have served and, with identified improvements, should provide a realistic and affordable level of protection. Outlying buildings

represent a particular weakness and should be phased out as quickly as possible after the new building is habitable. After completion of the new building, the matter of protection against terrorist attack should be revisited. Protection of one compound permits concentration on enhanced security procedures that is not possible with a system of diverse and decentralized quarters.

In conclusion, the threat is recognized as is the reality that the good fortune generally enjoyed by domestic Agency facilities does not preclude future violence. Plans are in existence to deal with terrorist attacks which in the main reflect dependence on Federal and local law enforcement agencies to respond and act. Our current physical security precautions leave room for improvement and those considered feasible and appropriate have been cited. We take comfort without smug satisfaction that in-place safeguards are considerably more stringent than those found in almost all of Government, and that these safeguards have done the job given a benign environment. We eschew the fortress mentality and appreciate a degree of risk must be accepted in an open society. To reduce the risk, we recommend suggested enhancement be implemented and that other reasonable safeguards be examined in future when a centralized operation will permit greater control of the Headquarters compound. Immediate action should be directed toward a visitor control center, by far the paramount need. In the meantime, we plan to maintain productive liaison with Federal and local police agencies that must supplement our own limited resources and authority.

OVERSEAS

Based on trends established in the late 1960's and continued throughout the 1970's, terrorism can be expected to continue at least at the same levels and perhaps even to increase throughout the 1980's. Of more specific concern is the fact that terrorism continues to target Americans and American installations as symbols of U.S. "Imperialism." Until the mid 1970's, more than half of all Americans killed by terrorists were killed only because they were coincidentally at the location of an attack. Since 1978, however, terrorists have tended specifically to target Americans. This trend continued during the period 1980 - 1982 with 21 U.S. citizens dying as a result of international terrorist incidents with 15 of these individuals being specifically targetted. A total of 385 terrorist incidents were recorded as directed against American citizens or property in 1982 alone. 30 of these resulted in casualties. U.S. diplomats were primary victims of terrorist incidents, accounting for approximately 38 percent of the total, while U.S. military personnel were the victims of approximately 18 percent of the terrorist incidents aimed at Americans in 1982. Since almost all

[redacted] 25X1

they obviously must be considered prime targets for terrorism even without taking into account the added dangers associated with their Agency duties.

Since the mid 1970's, the Office of Security has been responsible for a comprehensive personnel protection program. This program is designed to reduce the liklihood that a security conscious individual will be the target of a terrorist incident in the first place and to reduce his vulnerability in the event he is targetted despite his security consciousness. The objective of the program is to reduce the risks of attack by providing individuals and command elements with knowledge of countermeasures which can be used to detect, neutralize, or evade terrorist/criminal attacks. The Office of Security's personnel protection program consists of the following:

° Briefing and training programs for employees and dependents who are about to be transferred overseas.

° Surveys by personnel protection specialists at overseas locations.

25X1

Up until FY 1983 funding for personnel protection equipment and installations was obtained from area divisions. In FY 1983 over two million dollars was allocated in the OS budget for the enhancement of our overseas personnel protection program. This money is being used to upgrade emergency communications equipment; to install alarm systems, locking devices, security grillwork, etc., in residences; and for vehicle and body armor. Approximately $500,000 of these funds is being used for safety equipment both in residences and offices. In following years, it is anticipated that at least $100,000 will be funded to enable us to maintain our basic personnel protection capability. This continued funding is required since facilities and residences are constantly changing and security equipment requirements arise after each change. In cases such as vehicle armoring, the equipment is perishable and must be replaced periodically.

Funding must continue at a level adequate to enable us to keep our personnel protection profile up-to-date. This funding must include both office equipment and residential equipment. Typical items funded under this program would be emergency destruction equipment, vault doors and escape hatches, emergency power upgrades, grilles and locking equipment for residences, residential alarms, and vehicle and body armor. (Emergency communications equipment must also be continually upgraded but responsibility for this requirement should most logically be handled by the Office of Communications). The training of our personnel in personnel protection, residential security, defensive driving and emergency destruction needs to be continued. Staffing of OSSB must take into account the need to

meet these training requirements. As an alternative, the security staff [redacted] could be expanded to include an officer who would be responsible for handling these requirements. 25X1

In addition to the aforementioned equipment and training needs, there is a further need for the Office of Security to be in a position to provide timely responses to emergency situations. Our current staffing is geared to maintenance of a once every two years survey schedule. Personnel protection is one of the elements covered during these surveys. However, each emergency or priority personnel protection requirement impacts negatively on the maintenance of even this minimum schedule. The most effective way to provide an adequate response capability would be through the positioning of additional Agency security professionals at various locations overseas. For example, the Regional Staffs in Europe, East Asia and Africa should be expanded by at least one individual and Regional Staffs should be established for Latin America and the Middle East.

Next 5 Page(s) In Document Denied